CEO Update: Asset Protection's Revolutionary Steps p. 25

A CAHNERS PUBLICATION

MAY 1991

SECURITY®

THE MAGAZINE FOR SECURITY DECISION MAKERS

HIGH SECURITY p. 26

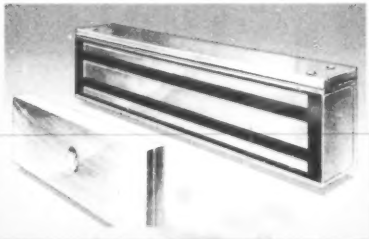
Checking Out The Bosses p. 30

Ways to Squeeze More Out of Reports p. 37

Five Monitor Buying Tips p. 39

Finally: Industry Action on False Alarms p. 43

Equipment Focus: Electromagnetic Locks p. 48



Stephen Fitzgerald
General Manager
John Hancock Center

SECURITY®

THE MAGAZINE FOR SECURITY DECISION MAKERS

A CAHNERS PUBLICATION/VOLUME 28, NUMBER 5/MAY 1991

DEPARTMENTS

9 Editorial/Masthead

10 Security Indicators
Security takes on fire code compliance. Private security may handle alarm response within the next 5 years.

13 Idea Exchange
Safety committee initiates routine inspection of school playground equipment to reduce the chances of accidents and lawsuits.

Formal inspection of playground equipment becomes a priority. (p. 13)

19 Issues
Effective security requires alert and committed top management support.

FEATURES

25 REVOLUTIONARY CALL FOR ASSET PROTECTION MANAGEMENT
Chief executive officers seek security programs that reflect to the bottom line.

26 Cover Story
HIGH SECURITY
Life safety and security at the architecturally famous John Hancock Center stresses personable attention, thanks to security-savvy property manager.

Mixed-use property at the John Hancock Center has complex security needs. (p. 26)

30 KEEPING THE PIECES TOGETHER
High-level job candidates may not complete job applications; background checks minimize white collar crime.

37 SYSTEM REPORTS: 5 WAYS TO DO MORE
Security decision makers can squeeze more out of reports to solve problems and identify trends.

39 DON'T FORGET THE MONITOR
A monitor plays an integral part in the CCTV picture. Review these tips to meet your specific needs.

On the Cover
Property management professionals are more knowledgeable of the benefits of security, like Stephen Fitzgerald, who has security responsibility at one of the world's tallest multi-use buildings. (p. 26)

SERVICES

43 Industry Strives to Reduce False Alarms
The alarm industry — vendors and associations — strive to defeat the false alarm problem.

EQUIPMENT FOCUS

48 Low-Maintenance Electromagnetic Locks Protect Entrances with Fail-Safe Force
Electromagnetic locks protect against intrusion and release their hold in life-threatening situations.

53 Product Update

Best Lock's newly introduced cylindrical lock is one of more than a score of hot products inside this month. (p. 53)

63 Literature

64 Classifieds

67 Reader Service Cards

Cahners Publishing Company, A Division of Reed Publishing USA ☐ Specialized Business Magazines for Building & Construction ☐ Research ☐ Technology ☐ Electronics ☐ Computing ☐ Printing ☐ Publishing ☐ Health Care ☐ Foodservice ☐ Packaging ☐ Environmental Engineering ☐ Manufacturing ☐ Entertainment ☐ Home Furnishings ☐ and Interior Design. Specialized Consumer Magazines for Child Care ☐ Boating ☐ and Wedding Planning.

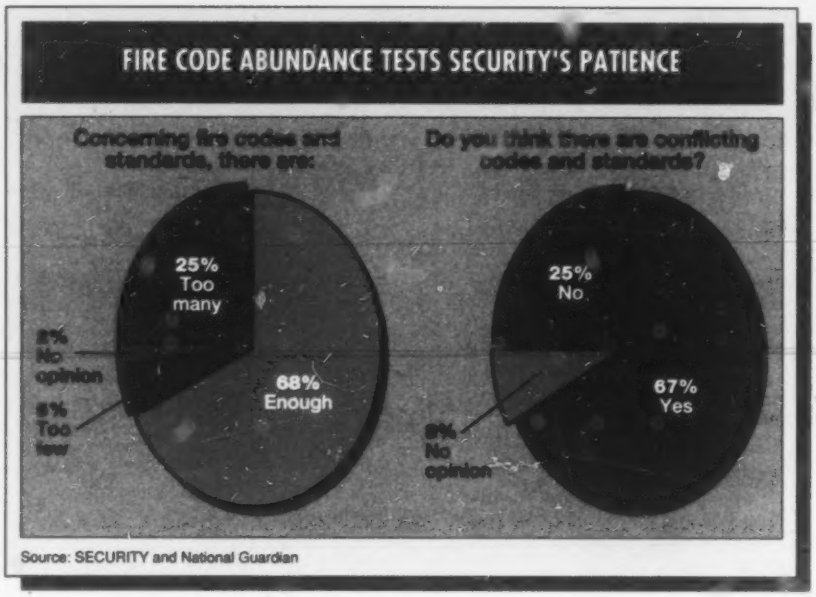
SECURITY (ISSN 0890-8826) (GST #123397457) is published monthly, except for March and August when two issues are published in national and separate editions, by The Cahners Publishing Company (Subscription includes all issues). Cahners Publishing Company is a Division of Reed Publishing USA, 275 Washington St., Newton, MA 02158-1630. Terrence M. McDermott, President; Frank J. Sibley, Executive Vice President; Charles E. Moodhe, Senior Vice President/General Manager, Chicago Division; Jerry D. Neth, Senior Vice President/Publishing Operations; J.J. Walsh, Senior Vice President/Finance; Thomas J. Dellamaria, Senior Vice President/Production and Manufacturing; Ralph Knupp, Vice President/Human Resources. Circulation records are maintained at Cahners Publishing Company, 44 Cook St., Denver, CO 80206-5800. Phone: 303/388-4511. Second-class postage paid at Denver, CO 80206-5800 and additional mailing offices. Postmaster: send address corrections to *SECURITY* P.O. Box 173377, Denver, CO 80217-3377.

SECURITY copyright 1991 by Reed Publishing USA; Ronald G. Segel, Chairman and Chief Executive Officer; Robert L. Krakoff, President and Chief Operating Officer; William M. Platt, Senior Vice President.

Annual subscription rates for non-qualified people: USA, $59.95; Canada/Mexico, $89.95; other countries, $115 for surface mail and $165 for air mail. Single copies are available for $10, $14 and $18 (USA, Canada/Mexico and foreign). Product source guide is available for $50. Please address all subscription mail to *SECURITY*, 44 Cook St., Denver, CO 80206-5800. *SECURITY* is a registered trademark of Reed Properties Inc., used under license.

SECURITY INDICATORS

Trends and forecasts for determining loss prevention needs.


FIRE CODE ABUNDANCE TESTS SECURITY'S PATIENCE
Concerning fire codes and standards, there are:
25% Too many
68% Enough
2% No opinion
5% Too few
Do you think there are conflicting codes and standards?
25% No
67% Yes
8% No opinion
Source: SECURITY and National Guardian

Most decision makers say there are enough, too many or conflicting fire codes. The NFPA says technical requirements among code-writing bodies are very similar.

FIRE PREVENTION

Cited: Code, Standard Conflicts Amid Expanding Fire Guidelines

Keeping up with the ever-increasing number of fire codes and standards is becoming more challenging for security decision makers.

More than two-thirds of respondents to SECURITY's 1991 First Quarterly Telephone Survey say the current number of fire codes and standards is on target. One quarter, however, say there are too many codes and standards. Fifty percent of those who cite code overkill represent retail establishments. Just five percent say there are too few codes; institutions are most seeking additional guidance through fire codes. SECURITY survey respondents demographically reflect the entire security decision-making population.

The majority of SECURITY's survey respondents agree that code-making organizations author conflicting codes and standards. Once again, retail voices highest discontent. Nationwide retail chains, especially, are challenged by ambiguities among code-making bodies and varying state codes.

The National Fire Protection Association (NFPA), Quincy, Mass., one of several code-making bodies, has authored 275 fire codes and standards. Arthur E. Cote, NFPA's assistant vice president and chief engineer, says amendments written at state and local levels account for further confusion among safety-conscious businesses.

"Unique geography and fire defense circumstances trigger the need for code differences among municipalities," Cote tells SECURITY. "A manufacturer may have to build or transport its products differently for some states."

NFPA is frequently petitioned to develop codes and standards for new business areas, according to Cote. "Business sectors today — more than in the past — are asking us for guidance," he says.

CODE MANAGEMENT

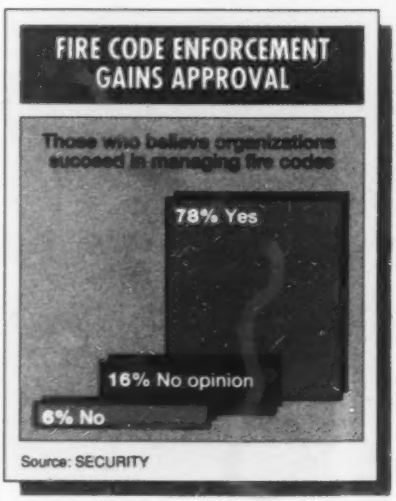
Fire Code Organizations Gain Thumbs-Up

The majority of security decision makers say they're expected to comply with too many fire codes and standards. Nevertheless, the organizations which write the codes score high marks among respondents to SECURITY's 1991 First Quarterly Telephone Survey.

Among respondents, 78 percent say organizations dedicated to fire prevention successfully manage fire codes and standards. Just six percent disapprove of organizations' management of codes.

Factory Mutual Engineering and Research (FME&R), Norwood, Mass., maintains 325 loss prevention guidelines, 200 of which are fire- or explosion-related. NFPA and FME&R spokespersons contend their organizations are working to narrow differences between codes.

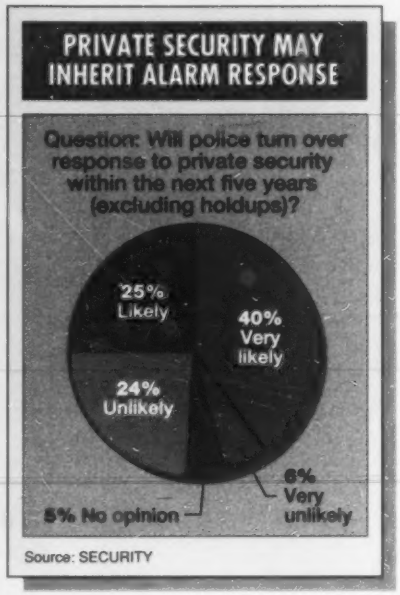
Larry Chase, vice president and standards division manager for Factory Mutual's Research Corp., tells SECURITY, "The emphasis is on keeping existing standards technically current. We are, however, developing new advisory guidelines targeted to newer business areas. Other new guidelines are intended to 'fill in some blanks.' "



Security endorses fire code management practices despite heavy code volume.

ALARM RESPONSE

Security Predicts Alarm Response Acquisition


PRIVATE SECURITY MAY INHERIT ALARM RESPONSE
Question: Will police turn over response to private security within the next five years (excluding holdups)?
25% Likely
40% Very likely
24% Unlikely
6% Very unlikely
5% No opinion
Source: SECURITY

Alarm response will be among private security's tasks by the mid-1990s, the majority agree.

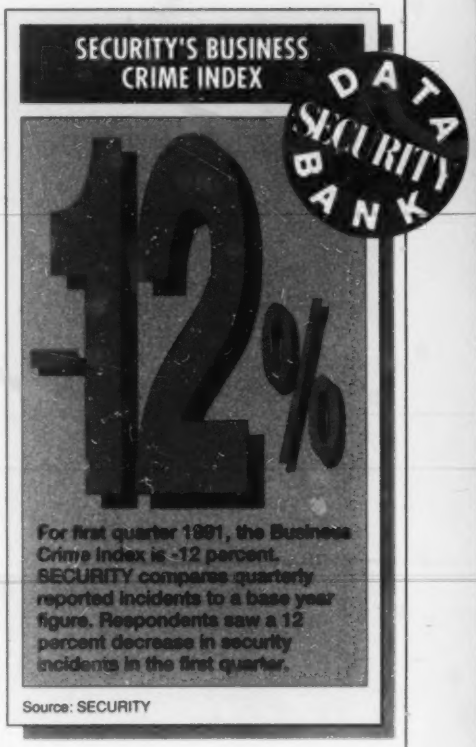
The debate over who should respond to alarms will continue as long as false alarms divert local police from priority tasks.

Private security — instead of police — will be expected to respond to alarms within the next five years, says a recent SECURITY survey. Among respondents, 65 percent believe it's likely or very likely that private security will follow up on non-holdup alarms by 1996.

Private security anticipates an increasing alarm response role as police tackle community problems aggravated by drug abuse. As recently as 1987, *Security Distributing & Marketing* reported that most police departments were not considering a no-response policy despite the financial and personnel drain triggered by frequent false alarm response. No-response policies give police the option to regard an organization's alarms as low priority after the facility has accumulated a specified number of false alarms within a specified period.

Among SECURITY survey respondents, 42 percent say false alarms are a problem for their organizations. The good news: 60 percent of those who cite this problem say it's lessening. Improved training can make the difference: 43 percent say inadequate user training is the primary false alarm cause.

BUSINESS CRIME INDEX


SECURITY'S BUSINESS CRIME INDEX
DATA SECURITY BANK
-12%
For first quarter 1991, the Business Crime Index is -12 percent. SECURITY compares quarterly reported incidents to a base year figure. Respondents saw a 12 percent decrease in security incidents in the first quarter.
Source: SECURITY

First Quarter incidents declined.

HUMAN RESOURCES

Hotline Prompts Employee Mistreatment Accusations

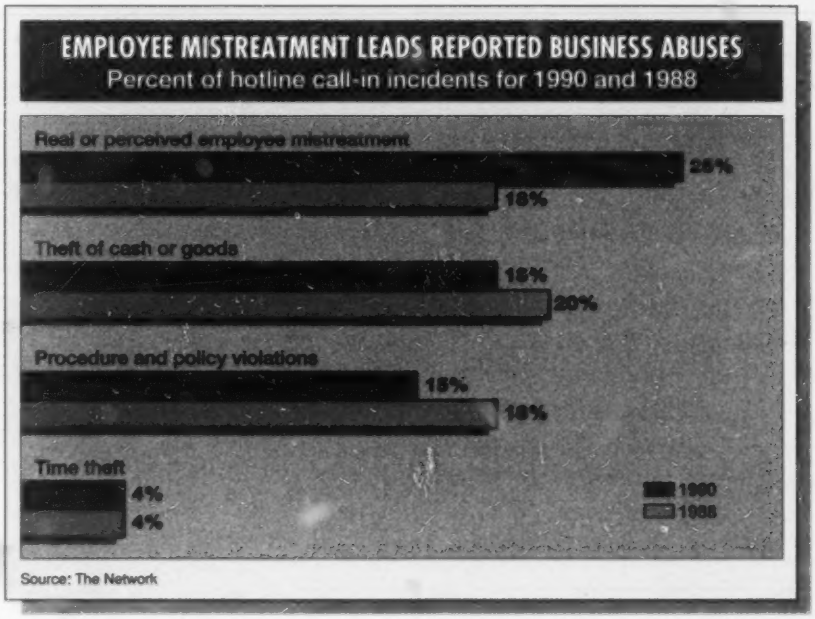
Employers, employees, vendors and customers tell it like it is when they have the chance to remain anonymous.

So says a survey conducted by The Network, a Norcross, Ga.-based publisher of awareness and training programs. The Network maintains the Information Clearinghouse, an anonymous toll-free number reporting program used by awareness program clients.

Real or perceived employee mistreatment tops theft and procedure violations as the most common business abuse reported by employees, employers or the public. The Network defines business abuse as any act that harms a company, its employees or its customers.

The Network's security awareness programs are targeted at improving communication between management and employees. Employees — the group that initiates most hotline calls — are encouraged to make an effort to work out problems with supervisors before calling the Information Clearinghouse. It's no surprise, consequently, that employee mistreatment claims are most often registered.

"Companies are starting to recognize that addressing security means addressing human resource issues as well," says Ed Stamper, president, The Network. "As a subscriber's loss prevention program becomes increasingly effective, the Information Clearinghouse receives fewer calls from that client."



Employee mistreatment leads reported business abuses for 1990. Time theft, equal opportunity violations and courtesy problems remained relatively stable since 1988.

Keeping the Pieces Together

Through careful executive screening, security decision makers fortify the workplace against white collar crime.

By Rebecca D. Russell
Senior Editor

It may be old news, but when it lands on your doorstep, it's unwelcome. Newspapers are rife with stories that detail fraud, industrial espionage and embezzlement perpetrated by management-level personnel at companies large and small.

By the time the headlines break, senior managers have asked the tough question: How will the company protect against such damage in the future?

Security must answer.

Estimates peg the cost of economic crime at 2 percent of gross national product. Yet what does business do to prevent white collar crime?

Prevention-conscious decision makers need to take the offensive, identifying potential problems before executives fill out a W-2. The solution: preemployment screening of employees at all levels.

"More than 75 percent of the people who perpetrate white collar crimes did so at another company," says Eugene Ferraro, vice president, Krout & Schneider Inc., Los Angeles, an investigative firm.

Some 29 percent of resumes are fraudulent, says David Karas, marketing manager, Equifax Services Inc., Atlanta, another national investigative firm.

Ferraro and others contend that companies generally do less screening for higher-titled positions. Background checks "reveal so many gaps that the company would not have hired the person if he applied for janitorial work," he says.

Developing Corporate Support

Improved executive job candidate screening requires commitment from a cross-section of company departments: executive management, security, human resources, legal and audit.

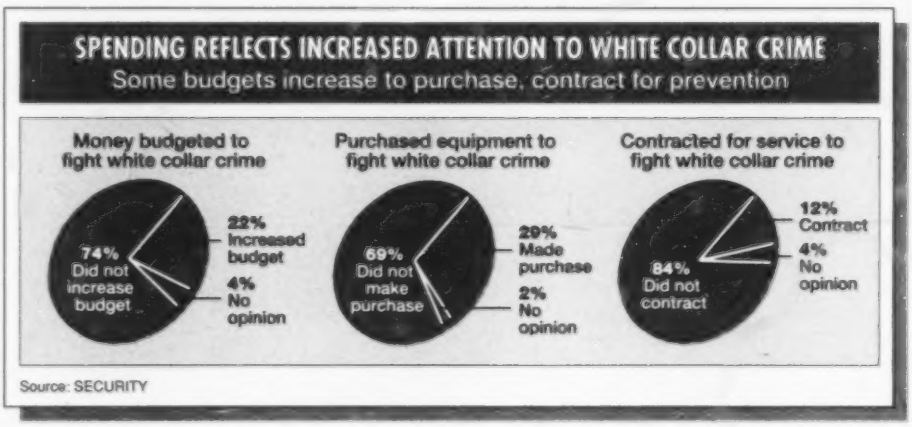
"White collar crime is generic to all industries. The difference lies in the methodology of hiring and screening and the work environment," says Tim Williams, assistant vice president of corporate security, Northern Telecom, Nashville, Tenn. "You have to look at how it fits into the overall employee environment. There's no quick fix."

Traditionally, business contracts with an investigative company to check a job candidate's background. Candidates sign a release form consenting to the check; pertinent information is forwarded to the screening company.

Companies can tap information that may be indicative of personal traits and levels of responsibility. Driving records may reveal a history of substance abuse or reckless driving. Criminal and civil court records show whether the person has been the object of a lawsuit or has initiated suits against a previous employer. Other searches include bankruptcy, tax liens and verification of social security number, address, education and previous employer. Some also check credit history to determine personal financial management.

"It is a piece in the whole puzzle," says Patrice McCall, human resource manager at the California regional headquarters of Inacomp Computer Centers, Garden Grove.

Lacking a security department to collect background information, Inacomp contracts with Krout & Schneider for 24-hour report turnaround. Following


SPENDING REFLECTS INCREASED ATTENTION TO WHITE COLLAR CRIME
Some budgets increase to purchase, contract for prevention
Money budgeted to fight white collar crime
74% Did not increase budget
22% Increased budget
4% No opinion
Purchased equipment to fight white collar crime
69% Did not make purchase
29% Made purchase
2% No opinion
Contracted for service to fight white collar crime
84% Did not contract
12% Contract
4% No opinion
Source: SECURITY

Business sees an increase in budgeting for purchases to combat white collar crime.

Executive Background Checks Help Limit Liability Tangles

interviews, a job candidate completes several employment tests. Krout & Schneider conducts subsequent background checks.

Gaining popularity is the introduction of computer networks, which allow businesses equipped with a computer and modem to gather applicant information on-line.

Robert Ayres, CPP, director of security at Merle Norman Cosmetics, Los Angeles, says security checks veracity of applications for all levels of jobs. He plugs into an on-line search through CDB Infotek, Orange, Calif.

Looking At Long-Term Costs

Elsewhere, a security manager at a defense contractor says he has two primary resources: criminal record microfiche on file in the security office and the CDB Infotek computer database.

"People applied for top financial positions and a check showed a history of embezzlement," the decision maker says.

Brad Feinberg, manager of assets protection at Christian Salvesen Distribution Services, Secaucus, N.J., contracted for background checks, but recently invested in hardware and software to handle this task in-house. Feinberg estimates that for three years he spent $250 per inquiry, for a total cost of $20,000. With an investment of close to $7,000 for hardware and software, he estimates long-term cost will be less than half of the outside costs.

"It is more cost-effective to do it ourselves. It will speed turnaround and the accessibility is incredible," he says.

While doing the job yourself may save up-front charges, it can infringe on staff time.

Tests Can Be Telling

Pre-employment tests are another screening choice for employees at all levels. Researchers at London House, Park Ridge, Ill., tested 111 high-level personnel who attended management-level seminars. Each attendee — 40 vice presidents and above, 66 mid-level managers and five non-managers — completed an ethics questionnaire and nine paper-and-pencil psychological tests.

"Executives and managers who scored above average on the ethics questionnaire tended to have a more realistic view of their role in the organization," says Alan J. Nerad, London House management assessment consultant. Tests can help identify if high-level employees may pursue unethical behavior, he says.

Screening Your Business Partners

Brian Jenkins, Kroll Associates, Los Angeles, says a variety of business market changes — the emerging global marketplace, ever-expanding information technology capabilities, increasing competition — have created a new criminal atmosphere.

"You used to do business with someone you had golfed with for 35 years; today you increasingly do business with strangers," Jenkins says.

"It is more cost-effective to do background checks ourselves."
— Brad Feinberg

Following this trend is an increase in vendor verification or vendor due diligence, says Don Walker, president, Business Risks International, Nashville. In-the-know businesses seek help to review the companies they do business with, to help eliminate future legal entanglements with potential white collar criminals.

Suzanne Jacaruso, vice-president/secretary, Sutton Associates, Hempstead, N.Y., says, "Most companies find that the effects of not doing background investigations costs them in legal fees and uncollected money."

It is this prevention mindset that prompts savvy security decision makers and business managers to explore background screening options. □

Executive Background Check Tips

If your organization has not tested the waters of background checks for execs, consider these tips.

First, develop a corporate strategy, suggests Tim Williams, assistant vice president of corporate security, Northern Telecom, Nashville, Tenn. This will help identify roles and avoid ambiguities as staff from several departments work together.

For specific department interaction, a defense contracting company security manager says mutual confidence between security and human resources is critical. "It is a lot of work to hire someone. Security can't just say, 'no, you can't hire this person.' Human resources has to be able to see that you are doing it on more than instinct."

If your business chooses to tap into on-line information retrieval, Robert Ayres, CPP, director of security at Merle Norman Cosmetics, Los Angeles, suggests learning about the following.

- Turnaround of information.
- Information quality guarantee: "Is what you get what they get?"
- Cost.
- Geographic areas covered.

Also be sure to talk with other users to identify strengths and concerns.

For More Information

Business Risks International	Circle 153
CDB Infotek	Circle 154
Equifax	Circle 155
Kroll Associates	Circle 156
Krout & Schneider	Circle 157
London House	Circle 158
Sutton Associates	Circle 159
U.S. Datalink	Circle 160

System Reports: 5 Ways to Do More

System report data helps security analyze the past and plan for the future.

By Brenda Moss
Staff Editor

Where is your security system report data right now?

It's likely the data resides in a file drawer. When an incident occurs, it's time to dig through stacks of paper — and point fingers.

Fire, access control, facilities management and electronic guard tour systems are among technologies which frequently sport report-generating capability. Following are five ways to get the most out of system reports.

1. Look for Trends

"People only refer to reports after something happens — they don't look for movement," says Harold Frank, CPP, owner, H. Frank & Associates, a Palm Beach Gardens, Fla.-based international consulting firm.

Frank suggests tracking after-hours employee access and excessive use of one person's access card or number. This is crucial when access systems don't employ time-zone lockout.

The person assigned to read system reports must be educated to identify problem areas, Frank adds.

2. Justify Security's Position

"Reports can show that security is working," says James Ryan, Phd., CPP, president, James H. Ryan Associates, Petersburg, Va. "They can also back up requests for additional funds."

3. Provide Instant Answers

Security stays in step with other departments by providing instant answers to access- and safety-related questions.

"A computer program allows for quick compilation of complex reports," says Denis O'Sullivan, CPP, president, PPM 2000, Blue Bell, Pa. PPM 2000 developed Security Intrack management software, which allows users to categorize incidents, analyze current data and forecast trends.

"People usually file system reports in a cabinet after an investigation," O'Sullivan says. "This data should remain part of an active electronic file to help predict future trends."

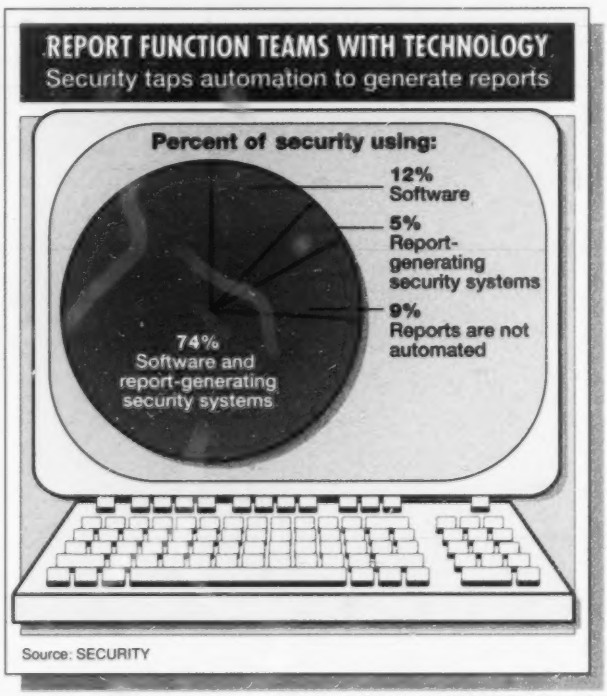
Systems which employ a processor with internal memory allow users to generate complete and "exception-only" reports.

"You usually don't need a day's complete activity on paper," says Ronald Libengood, CPP, principal security consultant, SecuraComm Associates, Pittsburgh. "Instead, store all data on a hard drive so you can retrieve it when necessary."

Users whose systems lack interrogation capability can export data from an access control system and import into a data base program, Libengood suggests.

4. Timely, Safe Advantages

User who employ facilities management systems tie safety and security system reporting functions — and reports — together. These systems also give security the chance to share time and attendance data with other departments.


REPORT FUNCTION TEAMS WITH TECHNOLOGY
Security taps automation to generate reports
Percent of security using:
12% Software
5% Report-generating security systems
9% Reports are not automated
74% Software and report-generating security systems
Source: SECURITY

Security looks to technology to generate reports.

5. Be Prepared For the Unexpected

Courtroom challenges demand complete system and incident reports. Security is ahead when reports are in the best possible condition.

Reports which contain full security disclosure help organizations obtain lowest-cost insurance coverage.

It takes both technology and security officers to give the complete picture when it comes to documenting incidents. Train officers to write clear, concise incident reports. □

For More Information

PPM 2000	Circle 170
Practical Education Services (Report-writing textbooks)	Circle 171
Proprietary Controls Systems Corp. (Facilities management and guard tour systems)	Circle 172